State of Colorado
Cyber Security Policies

Cyber Security Vendor Management

Overview

This policy document is part of the State of Colorado Cyber Security Policies, created to support the State of Colorado Chief Information Security Officer (CISO) in achieving the goals of the Colorado Information Security Act (C.R.S. 24-37.5, Part 4). All Agencies within the scope of this Policy must support and comply with the Requirements section of this document. Additional best-practice guidance is outlined in the Guidelines Section which has been designed to help a public agency achieve the objective of this Policy.

Authority

C.R.S. 24-37.5-401(1), C.R.S. 24-37.5-403(2)(e), C.R.S. 24-37.5-404(2)(b).

Scope

This policy document applies to every State agency ("Agency") as defined in C.R.S. 24-37.5-102(5). "State agency" means every State office, whether legislative, executive, or judicial, and all of its respective officers, departments, divisions, commissions, boards, bureaus, and institutions. "State agency" does not include state-supported institutions of higher education, the department of higher education, the Colorado commission on higher education, or other instrumentality thereof.

Policy

Agencies shall establish and maintain a Cyber Security Vendor Management Program that is to provide guidance regarding the selection of vendors, documenting terms of service delivery to include: confidentiality and non-disclosure agreements, security controls, measuring and reporting, and compromise disclosure in accordance with the policy requirements outlined below.

Definitions

For the purposes of this document, refer to C.R.S. 24-37.5-102, C.R.S. 24-37.5-402 and the Colorado Cyber Security Program Policy Glossary for any terms not specifically defined herein.

Roles and Responsibilities

Agency Information Security Officer (ISO) – is responsible for :

- Reviewing Agency RFPs and applicable purchase requests for appropriate security provisions.
- Reviewing Agency contracts for appropriate security provisions.
- Ensuring adequate statements are routinely added to the agency's procurement orders and other applicable purchase documents that do not require contracts.

Agency Executive Director – is responsible for ensuring that procurement and contracting processes meet this policy.

Agency Procurement Officer – is responsible for ensuring that the language meeting the requirements of this Policy is included in each vendor contract, purchase order or other applicable procurement document

Agency Chief Information Officer (CIO) – is responsible for completing periodic IT vendor performance reviews.

Requirements

The following are requirements under this policy:

Vendor Selection

Vendors must be selected according to C.R.S. 24-101-101 and the procurement rules R 24-101 through R24-112.

Vendor Contracts and Purchase Documents

Inter or Intra-agency IT service agreements:

If a public agency has an agreement with another public agency to provide IT services, the agency requesting service must ensure that the requirements under this policy are upheld by a Service Level Agreement or Memorandum of Understanding with the agency providing the service.

Statements of Work (SOW):

SOWs must clearly state the security requirements for the vendors to ensure that their work is consistent with state security policies.

SOWs must include a clear description of the scope of services provided under the contract or purchase order.

SOWs must clearly identify any and all types of sensitive data to be exchanged and managed by the vendor. Sensitive data is that which is determined to be Level 2 or higher by the public agency in accordance with the Data Handling and Disposal Policy, P-CCSP-011.

Purchase Orders:

Arrangements to procure vendor services and/or products that involve the exchange of sensitive information should be executed by a contract via the state controller's office. In the event a contract is not a viable purchasing option and a purchase order is a more appropriate mechanism, an Exhibit or Special Provisions must be attached to the purchase order that contains provisions meeting all SOW and contract requirements in this policy.

Contracts:

Contracts that include exchange of sensitive data must require state confidentiality agreements to be executed by the vendor, must identify applicable State policies and procedures to which the vendor is subjected, and must identify security incident reporting requirements.

Contracts must clearly identify security reporting requirements that stipulate that the vendor is responsible for maintaining the security of sensitive data, regardless of ownership. In event of a breach of the security of the sensitive date the vendor is responsible for immediately notifying the agency and work with the agency regarding recovery and remediation. In addition, the vendor is responsible for notifying all Colorado residents whose sensitive data may have been compromised as a result of the breach..

Security reporting requirements in the contract must also require the vendor to report all suspected loss or compromise of sensitive data exchanged pursuant to the contract within 24 hours of the suspected loss or compromise.

Contracts must contain provisions requiring that vendors handling sensitive data for the state must meet the same personnel security standards as State employees as outlined in the Personnel Security Policy, P-CCSP-012.

Contracts must include formal sanctions or penalties for failure to meet the security requirements in the contract or purchase document.

Management and Oversight

Vendors are required to observe the Colorado Cyber Security Policies, as published and updated by the Office of Cyber Security. Exceptions may only be granted by the respective public agency CIO and must be documented and reported to the Office of the CISO.

Agencies shall ensure all contracts being renewed are updated with provisions supporting the requirements of this policy.

Reporting and Monitoring

Agencies shall provide the appropriate security reporting contact information to each vendor upon contract initiation, along with any reporting instruction specific to the respective public agency.

The public agency shall have the ability to inspect and review vendor operations for potential risks to the State of Colorado operations or data. This review may include a physical site inspection and an inspection of documentation such as security test results, IT audits, and disaster recovery plans.

Guidelines

This section describes best practices for meeting the objective of this policy.

Vendor Security Controls

In accordance with the requirement for vendors to comply with the Colorado Cyber Security Program, each vendor provides:

- Effectively deployed and administered firewalls
- Intrusion Detection with 24x7 alerting capability
- An individual or group responsible for Incident Response, available 24x7
- Access controls to enforce restrictions on a need-to-know basis
- Established and tested policies and procedures
- Contingency Plans and Disaster Recovery Plans
- Personnel background checks that have performed in accordance with the contracting state public agency's procedures and provides to the agency a pass/fail determination (as determined by the agency based on the characterization of the engagement)
- Security testing and evaluation process for security controls, to include regularly scheduled, at least annually, vulnerability assessments.
- Configuration settings required to maintain the system's security on the system itself and other State systems that interface with it.

In addition, vendors managing critical data for the State of Colorado are required to provide physical security through the use of an acceptable physical access system, established access policies and tested controls.

Vendor Reporting and Monitoring

All contracts shall require the vendor to produce regular reports focusing on four primary potential risk areas:

- Unauthorized systems access
- Compromised data
- Loss of data integrity
- Inability to transmit or process data

Any exceptions from normal activity are to be noted in the reports, reviewed and the appropriate responses determined.

Vendor Termination

Upon termination of vendor services, contracts must require the return or destruction of all State of Colorado data in accordance with P-CSPP-008, Access Control Policy. State contract or

procurement managers are to immediately ensure termination of all access to State information systems and facilities housing these systems in accordance with the Physical Security Policy, P-CCSP-010.

References

- National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, "Recommended Security Controls for Federal Information Systems"